In the claims:

Following is a complete set of claims as amended with this Response.

1. (Currently Amended) A method comprising:

receiving first and second encryption keys from a key server;

receiving encrypted video from a broadcast video source; ~~source~~

generating a first cipher stream based on the ~~a~~ first key for decrypting the encrypted video;

generating a second cipher stream based on the second key to re-encrypt the decrypted video;

simultaneously decrypting and re-encrypting the encrypted video using a combination of the first and the second cipher streams;

conveying the re-encrypted video to a display device to be decrypted by the display device using the second key.

2. (Previously Presented) The method of Claim 1, wherein simultaneously decrypting and re-encrypting the encrypted video comprises exclusive OR-ing the encrypted video with the cipher stream combination.

3. (Original) The method of Claim 1, wherein the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams.

4. (Original) The method of Claim 3, wherein the first key and the second key have symmetric agreement.

5. (Previously Presented) The method of Claim 1, wherein receiving the first and second encryption keys comprises receiving one or more of the first key and the second key over a secure authenticated channel.

6. (Original) The method of Claim 5, wherein receiving a key over a secure authenticated channel comprises receiving the key from a sales server.

7. (Original) The method of Claim 5, wherein the secure authenticated channel comprises an Internet connection.

8. (Original) The method of Claim 5, wherein the secure authenticated channel comprises a telephone line.

9. (Previously Presented) The method of Claim 1, further comprising conveying the second key to the display device to enable the display device to decrypt the re-encrypted video.

10. (Previously Presented) The method of Claim 1, wherein the encrypted video is publicly available and encrypted with a public key and wherein the first key is a locally available private key.

11. (Previously Presented) The method of Claim 1, wherein the encrypted video is a broadcasted entertainment program.

12. (Currently Amended) An apparatus comprising a tangible ~~A~~ machine-readable medium having stored thereon data representing sequences of instructions which, when executed by a machine, cause the machine to perform operations comprising:

receiving first and second keys from a key server;

receiving encrypted video from a broadcast video source

generating a first cipher stream based on the ~~a~~ first key for decrypting the encrypted video;

generating a second cipher stream based on the ~~a~~ second key to re-encrypt the decrypted video;

simultaneously decrypting and re-encrypting the encrypted video using a combination of the first and the second cipher streams;

conveying the re-encrypted video to a display device to be decrypted by the display device using the second key.

13. (Previously Presented) The medium of Claim 12, wherein the instructions for simultaneously decrypting and re-encrypting the encrypted video comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising exclusive OR-ing the encrypted video with the cipher stream combination.

14. (Original) The medium of Claim 12, wherein the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams.

15. (Original) The medium of Claim 12, wherein the first key and the second key have symmetric agreement.

16. (Previously Presented) The medium of Claim 12, wherein the instructions for receiving first and second keys comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising receiving one or more of the first key and the second key over a secure authenticated channel.

17. (Previously Presented) An apparatus comprising:

a content interface to receive encrypted video from a broadcast video source;

a key interface to receive first and second encryption keys from a key server;

a computing device to generate a first cipher stream based on the ~~a~~ first key for decrypting the encrypted video, to generate a second cipher stream based on a second key

to re-encrypt the encrypted video and to simultaneously decrypt and re-encrypt the received encrypted video using a combination of the first and the second cipher streams; and

a sink interface to convey the re-encrypted video to a display device to be decrypted by the display device using the second key.

18. (Original) The apparatus of Claim 17, further comprising a secure authenticated channel interface to receive one of either the first key or the second key.

19. (Previously Presented) The apparatus of Claim 17, wherein the first key and the second key have symmetric agreement and wherein the combination of the first and the second cipher streams is a result of exclusive OR-ing the encrypted video with an encryption stream.

20. (Previously Presented) The apparatus of Claim 17, wherein the computing device conveys the second key to the display device to enable the display device to decrypt the re-encrypted video.

21. (Original) The apparatus of Claim 17, wherein the computing device includes a broadcast entertainment set-top box.